An Integrated Risk Management Framework

- The Triple-Triplet Concept for Risk-informed S&MA Management

Feng Hsu, Ph.D.

NASA GSFC CODE-170

NASA PM Challenges 2006

March 2006, Galveston TX

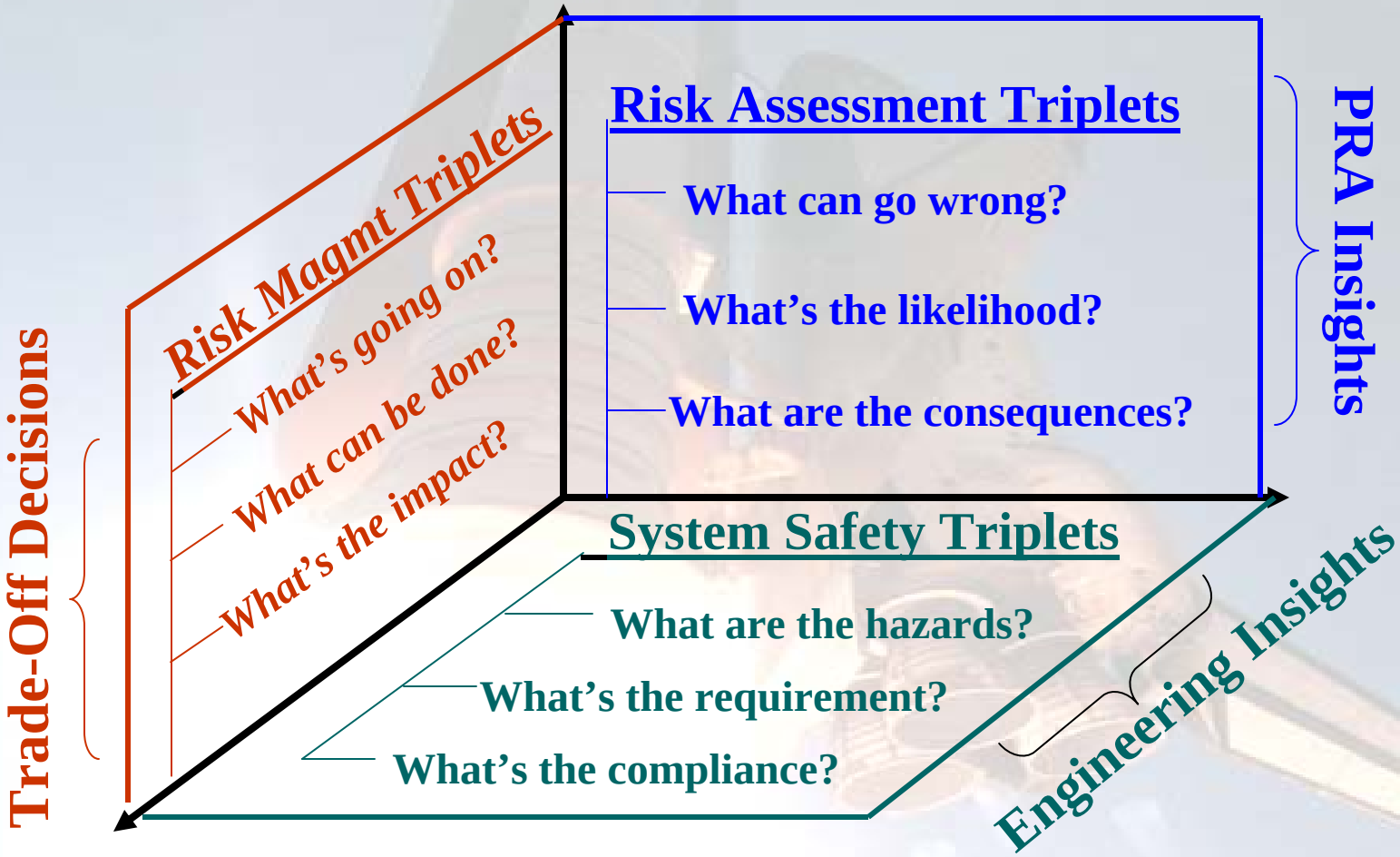
Why An Integrated Risk Management Framework Is Important?

- **A resolution to S&MA issues as pointed out in the CAIB report:**
  - **"Risk information and data from hazard analysis are not communicated effectively to the risk assessment and mission assurance process …"**
  - **"System safety engineering and management is separated from mainstream engineering …."**
  - **"Over the last two decades, little to no progress has been made toward attaining integrated, independent, and detailed analysis of risk …."**
  - **No process addresses the need to update hazard analysis when anomalies occur."**
  - **Need of "a disciplined, systematic approach to identifying, analyzing, and controlling hazards …"**
- **The complexity of STS and its successful operation necessitates an integrated total S&MA management process**
- **Hazard, Risk and Safety are integral elements to comprehensive S&MA management of any complex engineered systems.**
- **Need of An Integrated Process for Combining Hazard Analysis with PRA for Total Safety and Risk Management (can't be separated!)**
- **Utilization of A Systems Engineering Approach (closed loop system)**

Why An Integrated Risk Management Framework Is Important? (Cont'd)

- **The New Reality & Challenges for NASA**
  - **Fundamentally new**
  - **Greater Complexity**
  - **Multifaceted**
  - **Public Scrutiny**
  - **Uncertainty**

A Triple-Triplets ("Double T") Concept for An Integrated S&MA Management Framework



Conceptual Differences of System Hazard, Risk, Safety, Reliability:

HAZARD - System threat existed that can cause potential damage & harm. A necessary condition for risk but not absolute condition for risk or damages.

RISK - A integrated measurement of consequence of a undesired event occurrence. Not necessarily a mathematically measurable quantity

SAFETY - Assurance or level of confidence in accident/damage prevention & control. The system safety concept is the application of systems engineering and mgmt to the process of hazard, safety & risk analysis to identify, assess & control associated hazards while designing or modifying systems, products, or services.

RELIABILITY - Assurances of expected proper functioning of equipment, systems, hardware or software component as well as human performances etc. Low reliability must induce high risk but low risk not necessarily come from high reliability.

The System Safety Triplets

- A Safety Engineering Process

1. **What are the hazards?**

   Failure source identifications **(hardware/software/human/organization/external)**

   Hazard analysis/Hazard ranking using risk index matrix (semi-quantitative FTA)

   FMEA/FMECA and CILs on root cause identification & initiator ranking

2. **What are the safety requirements & goals?**

   Develop safety requirements & goal - when & where to impose?

   What are the organizational hierarchy & assurance for hazard control?

   Process for ensuring reliability, maintainability, supportability & inspections

3. **What's the compliances & verification?**

   Safety audit & regulatory mechanisms **for compliance & verifications**

   Process for documentation control and hazard/risk communications

   Culture for two-dimensional (vertical/horizontal) Risk/Hazard communications

The Risk Assessment Triplets

- A PRA Process To Gain Risk Insights

1. **What can go wrong?**

   Risk identification **(for all credible & significant hazards)**

   Hazards & Initiating event identification

   Scenario development, enumeration and structuring

2. **What's the likelihood that it would go wrong?**

   Risk quantification & measurement

   Reliability & Data assessment

   Risk evaluation & uncertainty assessment

   Risk ranking & importance measures

3. **What are the consequences?**

   Risk mitigation & Damage assessment

   Failure & success criteria evaluations

The Tradeoff Decision Triplets

- A Risk-Informed Decision Process

1. **What's going on?**

   Trend Analysis **RM & Risk-based performance monitoring/evaluation**
   Indicator technology - quantitative/qualitative trend/time series assessment)
   Accident Sequence Precursor (ASP) identification & evaluations
   Data mining & statistical anomalies/near-miss assessment
   Communication of issues & problems

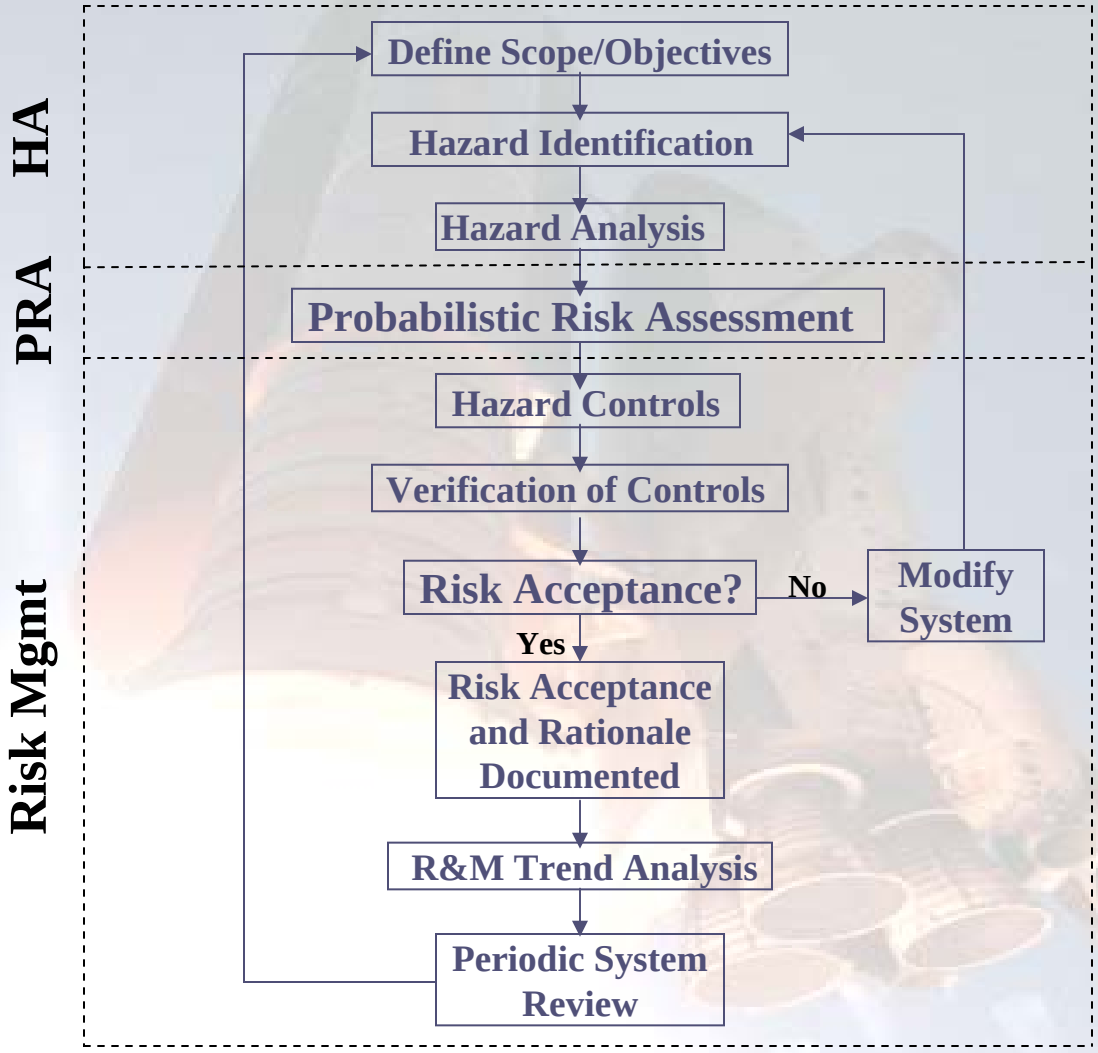
2. **What can be done?**

   Trade-off studies **using insights from both PRA & Hazard Analysis (HA)**
   What options are available & what are their associated trade-offs?
   Multi-objective, optimized cost-benefit analysis (CBA) & decision making

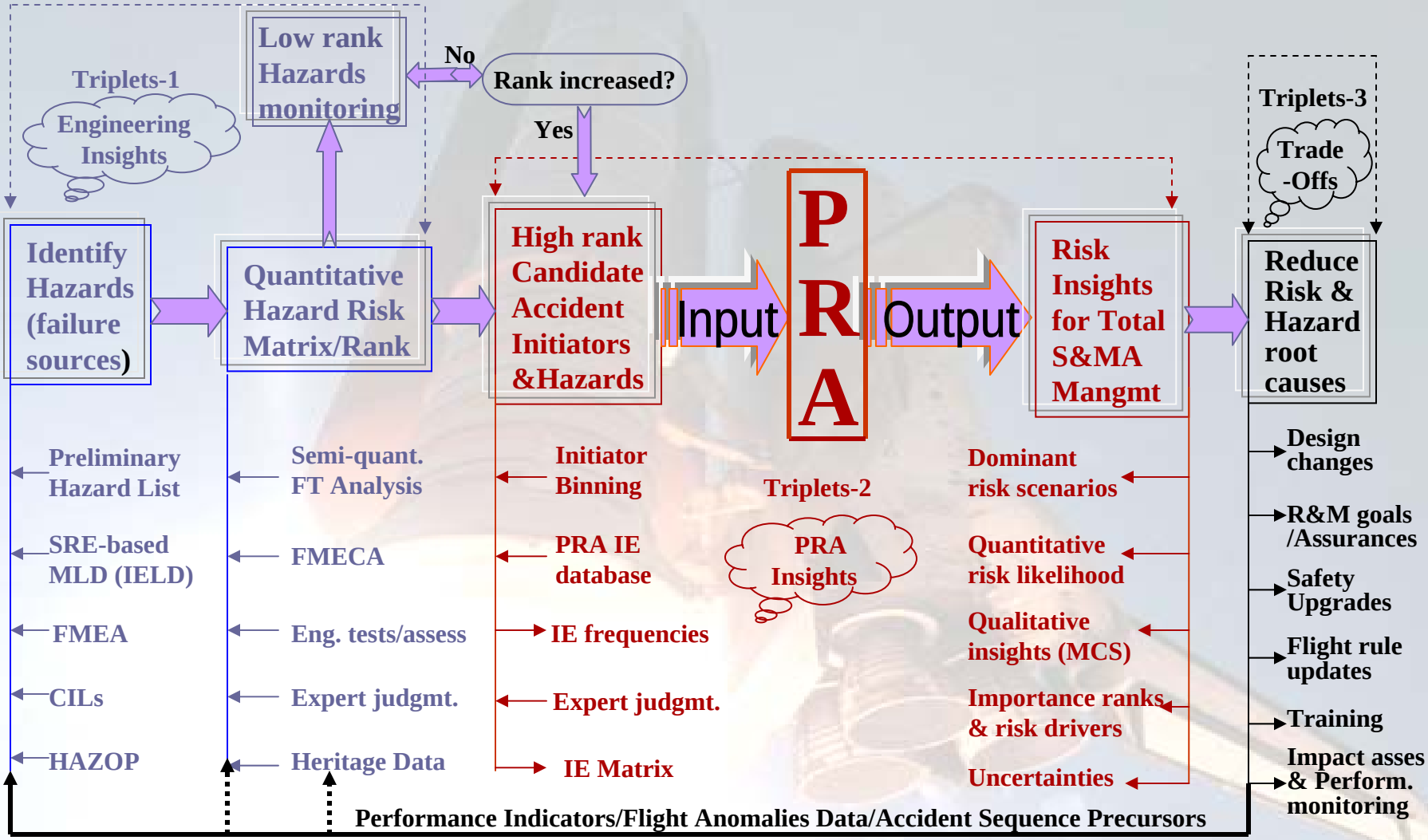
3. **What's the impact?**

   Impact assessment **of current mgmt decisions on future options (risk reduction)**
   Impact of risk control evaluations of risk mgmt activities on safety improvement

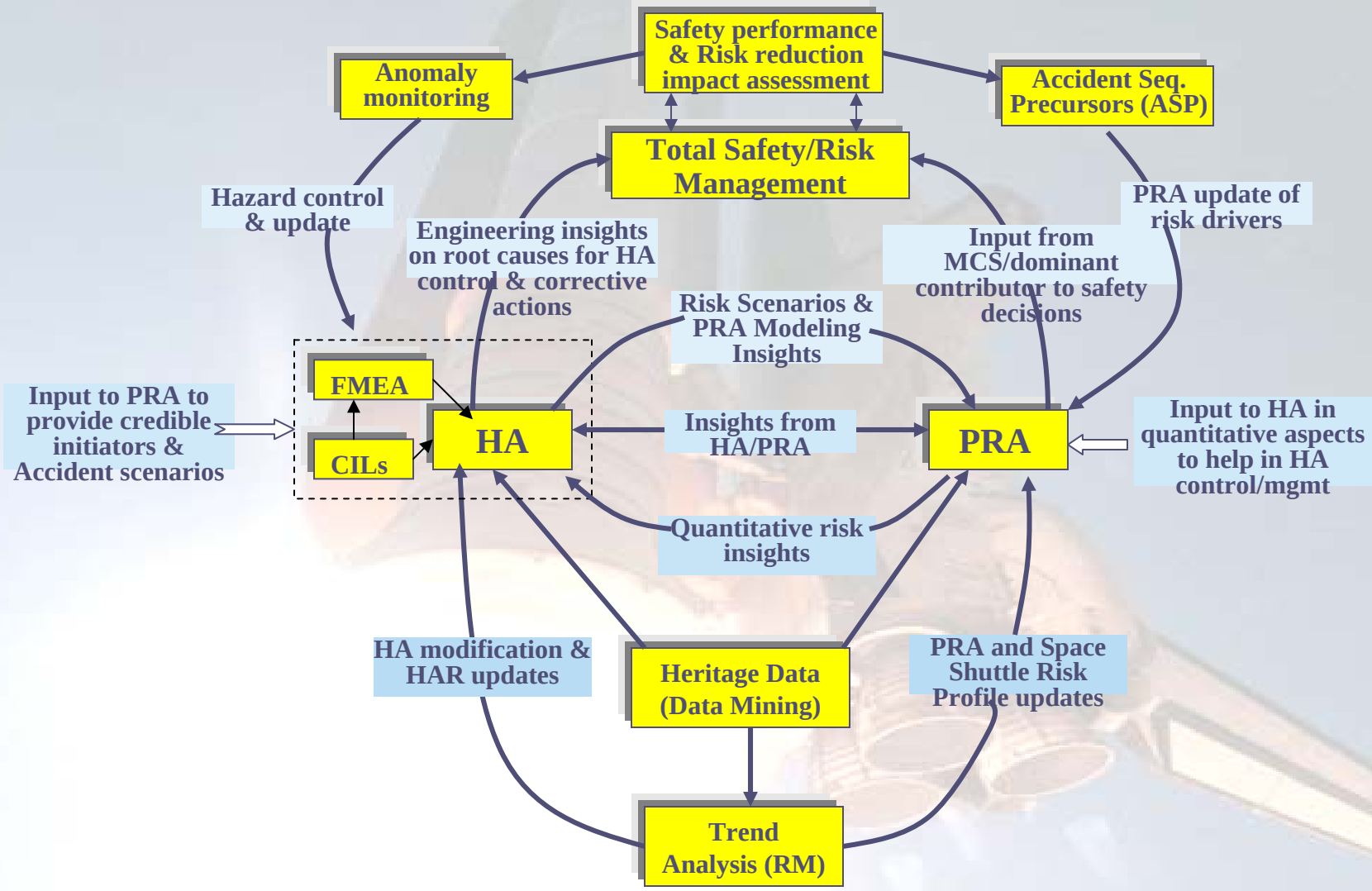
A Simplified Example Systems Engineering Process



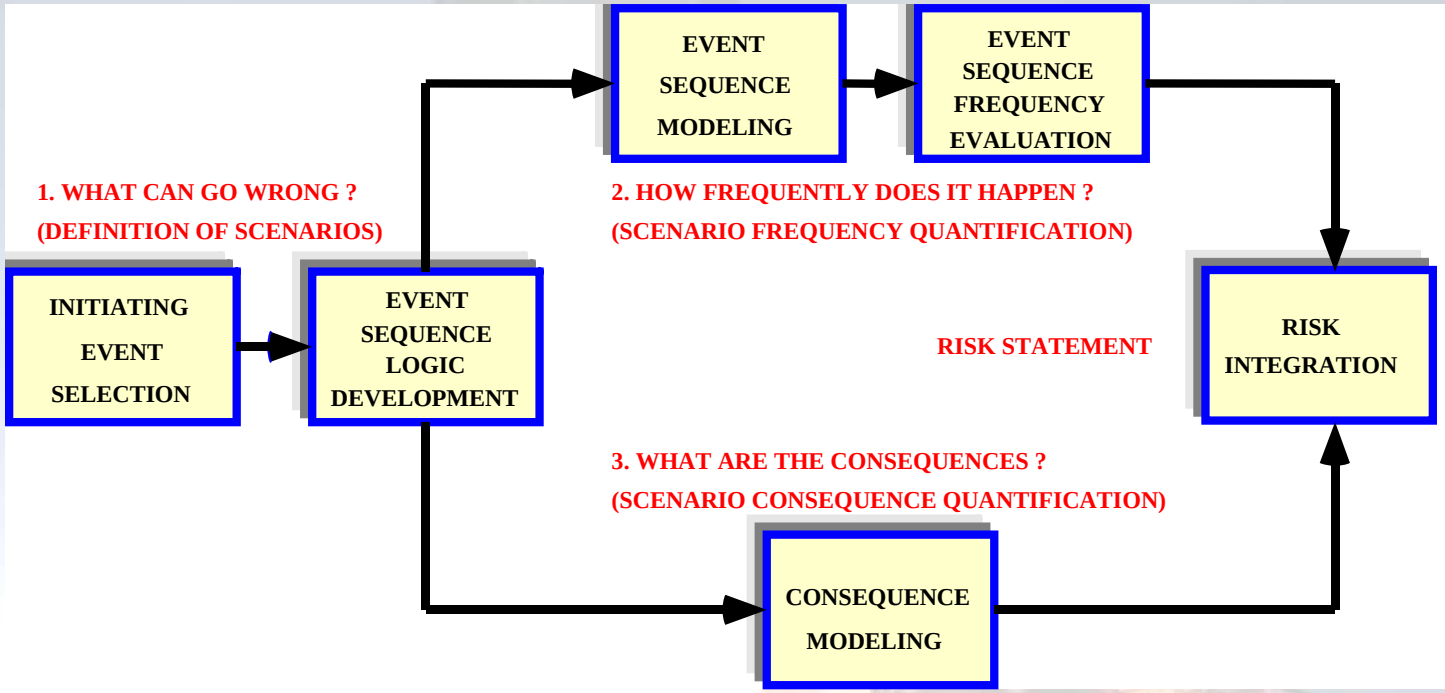
- Role of HA & PRA in the "Double-T" S&MA Mgmt Process



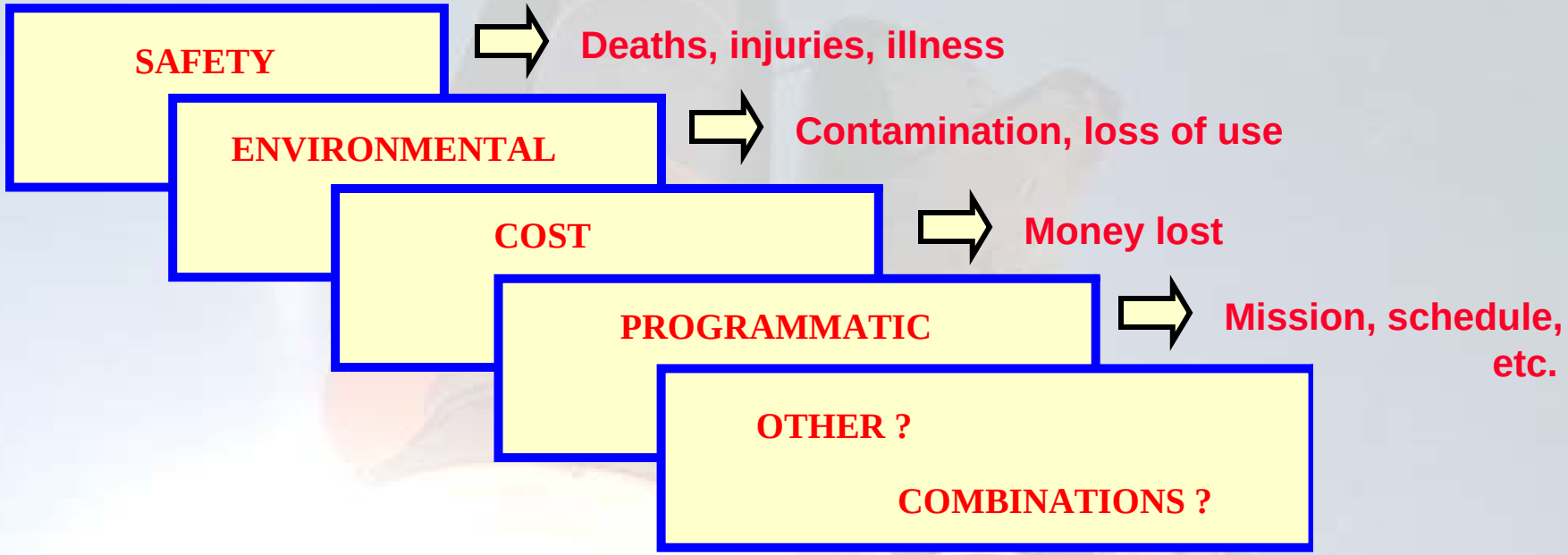
- An Integrated Process for Combining Hazard Analysis with PRA for Total Safety and Risk Management



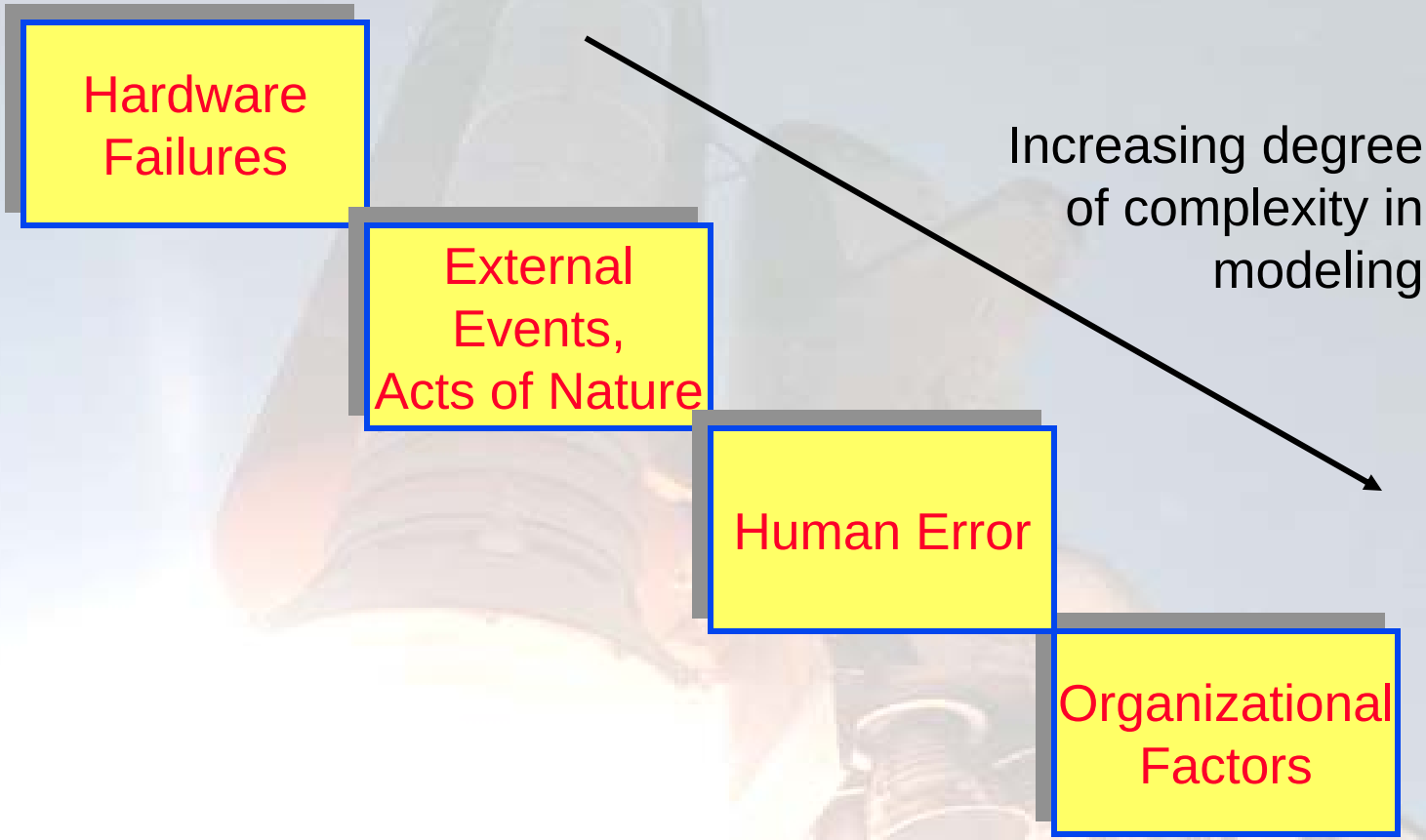
PRA Simply Described



Types of Risk and Related Consequences



Risk Sources in Safety Risk Assessment



Risk Assessment & Management

Inputs

- Mission Success Criteria
- Technical Data
- Cost
- Schedule
- Management Procedures
- Other

Improved Safety & Performance

Qualitative Risk Assessment

- FMEA
- FTA

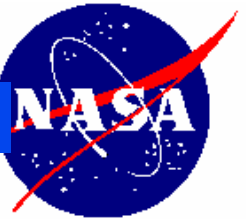
Quantitative Risk Assessment

- Initiating Events
- Scenario Modeling (MLD, ESD, ETA, FTA)
- Risk Quantification
- Uncertainty Evaluation

Benefits of PRA

Probabilistic Risk Assessment (PRA) has proven to be a systematic, logical, and comprehensive tool to assess risk (likelihood of unwanted consequences) in modern technological applications (e.g., nuclear power, electric power generation, chemical processing industry), for:

- ⇒ Improving system performance & mission success
- ⇒ Increasing safety in design, operation & upgrade
- ⇒ Saving money in design, manufacturing, assembly and operation



When Should PRA Be Performed?

- ⇒ When important decisions must be made about complex systems under uncertainty
- ⇒ When information is not sufficient to comprehensively assess strengths and weaknesses of complex systems by other means
- ⇒ When important complex jobs must be performed successfully for the first time
- ⇒ In all life cycle phases of a complex system

NASA Administrator's View on PRA

- ⇒ **July 29, 1996, the NASA Administrator, Dan Goldin:**
- ⇒ ***"Since I came to NASA [1992], we've spent billions of dollars on Shuttle upgrades without knowing how much they improve safety. I want a tool to help base upgrade decisions on risk."***
- ⇒ **Earlier "paper PRAs" prepared by NASA contractors would not serve the purpose.**
- ⇒ **October 1997, an early version of the NASA Quantitative Risk Assessment System (QRAS) is demonstrated to the Administrator.**
- ⇒ **February 1998, Version 1.0 of QRAS is baselined.**
- ⇒ **Two other intermediate version have been tested**
- ⇒ **March 2001, Version 1.6 of QRAS will be delivered. It will have full PRA capabilities.**

Space Shuttle

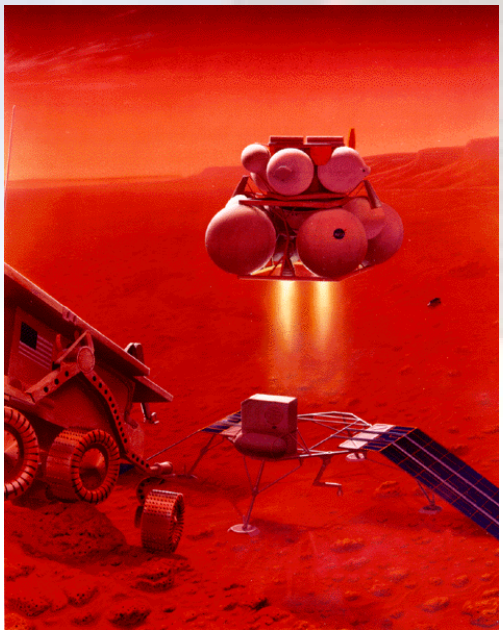
- Johnson Space Center and Marshal Space Flight Center have been modeling their Shuttle elements.
- Space Shuttle Program has begun to factor risk into their Upgrades Program.

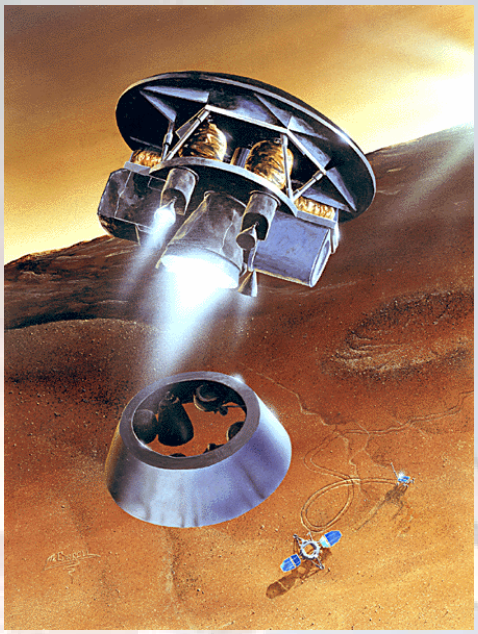
International Space Station

- ⇒ **1999 -- The NASA Advisory Council recommended, the NASA Administrator concurred, and the ISS Program has begun a PRA.**
  - » **First portion of PRA (through Flight 7A) delivered in Dec. '99; 2nd portion (through Flight 10A) expected in Dec. '00.**
  - » **Using the SAPHIRE software application for conducting PRA.**
- ⇒ **Objectives of ISS PRA:**
  - » **Provide a quantitative look at ISS operations risk**
  - » **Provide a model for future ISS safety decision-support activities**
  - » **Provide a model for safety related operations planning**
  - » **Provide a model for trading marginal safety enhancements versus cost**

Mars Sample Return Mission

- ⇒ **Mission must meet a Planetary Protection Program criterion of $<10^{-6}$ probability of Earth contamination upon return of sample**
- ⇒ **Use of PRA is being seriously considered as a means to evaluate mission compliance with the PPP criterion**





The Risk Management Picture at NASA

→ NASA Procedures and Guidelines 7120.5A, "NASA Program and Project Management Processes and Requirements," April 3, 1998

- Requires NASA Program & Project Managers to manage risk formally
- We are seeing evidence of real risk management in numerous NASA projects
- Risk management is a factor in high-level program/project decision-making

• "Continuous Risk Management" training course developed and pilot-tested on numerous NASA project teams

- To be picked up by NASA's APPL in FY 01

• Risk-Based Acquisition Management (R-BAM)

- Interim rule entitled "Risk Management," -- published in Federal Register June 14, 2000; effective July 14, 2000
- Changes NASA Supplement to the Federal Acquisition Regulations (FAR) to emphasize considerations of risk management in the acquisition process

Current PRA Status at NASA

- Strong interest and support for PRA
- In-house experience with traditional FMEA and some FTA

- Scarce and scattered PRA resources (people, tools, data)
- No corporate memory on PRA past work and data
- Inadequate communication and cooperation on PRA among Centers and with HQ

Suggested Objective For PRA

Develop a world-class *in-house* capability to perform, manage, and use Probabilistic Risk Assessment (PRA) methods at NASA

Ingredients for Success from Experience

- **In-house expertise** to perform, manage and use PRAs to make sound decisions
- **In-house ownership and corporate memory** of PRA methods, tools, databases and results
- **Lowest dependence** on outside help to manage, perform, understand, and use PRA methods and results to make management decisions